REMARKS

Claims 15, 19, 21 and 26 have been amended. Claim 18 has been cancelled. Claims 29 to 34 have been added. The remainder of the claims are unchanged.

Claims 15-24

The Examiner has rejected claims 15, 18, 19, 22 and 23 under 35 U.S.C 103(a) as being obvious in regard to U.S. Patent Publication No. 2003/0074590 (Fogle) in view of U.S. Patent Publication No. 2002/0129283 (Bates). The Examiner has also rejected claims 20, 21 and 24 under 35 U.S.C 103(a) as being obvious having regard to Fogle in view of Bates, in further view of U.S. Patent Publication No. 2005/0077997 (Landram) or U.S. Patent Publication No. 2005/0164720 (Huang). Amendments have been made to independent claim 15. The Applicant respectfully submits that amended independent claim 15 is allowable for the reasons set forth below.

Amended claim 15 recites a mobile device having a device lock module associated with the processor configured for:

> implementing a lock mode which places restrictions on user access to the mobile device if user input activity for the mobile device falls below a threshold,
>
> determining if the mobile device is in a secure location based on the determined location information,
>
> requiring input of a first predetermined password by a user to unlock the mobile device if it is in a secure location, and
>
> requiring input of a second predetermined password by a user to unlock the mobile device if it is not in a secure location.

Fogle discloses a device in which the device will enter a power-saving standby mode if a first predetermined time duration (T_A) goes by without user activity, and after entering standby mode, will subsequently enter a lock workstation mode in the event that a second predetermined time duration (T_B) passes without detection of a user input. Fogle does not describe nor suggest determining location information based on input signals received from the first input device, and changing the determined password required to remove the restrictions on user access in dependence on the determined location information, as acknowledged by the Examiner at page 3. The Examiner relies on Bates as disclosing this feature.

Bates discloses a method and electronic device such as a laptop computer or PDA having a GPS card and antenna. As described in paragraphs [0035], on power-up the electronic device determines its current location using the GPS card and antenna, determines a geographic-specific password for the current location of the device (based on a list of locally stored geographic-specific passwords for a series of geographic locations), prompts the user for a password, and compares the entered password against the determined geographic-specific password. If the password matches, normal processing continues. If the password does not match, the user is prompted to re-enter the password.

In amended claim 15, the password required to unlock the mobile device is based on whether the mobile device is determined to be in a secure location or an insecure location. The required password is not strictly limited to the geographic location, but the perceived security of the determined location of the mobile device. This is in contrast to Bates where the password required to unlock the device is a geographic-specific password. Furthermore, there is no description or suggestion in either Fogle or Bates for the feature of determining if the device is in a secure location based on the determined location information.

While Irvin (U.S. Patent No. 6,556,819) describes determining if the device is in a secure location based on location information, it does not describe applying different security settings depending on whether the device is in a secure location or an insecure location. In Ivrin, if the device is in a secure location, security features are disabled. If the device is not in a secure location, security features are enabled. This is in contrast to the claimed invention where different security settings are applied in relation to a particular security feature (i.e., different passwords) depending on whether the current location is determined to be secure or insecure.

Therefore, it is submitted that amended independent claim 15 is patentable in that the cited references fail to teach or suggest each and every feature recited. Claims 19-24 depend, either directly or indirectly, from claim 15 are patentable for at least the same reasons.

Claim 32

New claim 32 is similar to former claim 25 which was previously cancelled by the Applicant's amendment dated August 21, 2006 in order to expedite the allowance of the present application. As the Examiner has now withdrawn the allowance of claims 15, 18-24 and 26, and the subject matter of former claim 25 is not the subject of a continuation application, the subject matter of former claim 25 is being represented for reconsideration with some amendments thereto.

In the Office Action of April 21, 2006, the Examiner objected to claim 25 under 35 U.S.C. 103(a) as being unpatentable having regard to U.S. Publication Number 2003/0073448 A1 (Ozeki) in view of Bates.

New independent claim 32 is directed to a method for providing security to a mobile electronic device having a device lock function that restricts use of the mobile electronic device by locking the device under predetermined circumstances, the method including receiving input signals from an input device of the mobile electronic device, determining if the mobile electronic device is in a secure location based on the input signals; and requiring input of a first predetermined password by user to unlock the mobile electronic device if it is in a secure location and requiring input of a second predetermined password by user to unlock the mobile device if it is not in a secure location.

Ozeki discloses a device in which an access prohibiting unit 181 of the device prohibits access to memory when a condition verifying unit 15 of the device determines that the current location information does not meet the conditions for operation, and the prohibition cancellation unit 182 cancels the prohibition when the password pre-registered by the owner is input (see for example page 3 [0048]). In other words, Ozeki discloses a device in which user access is freely permitted until location information for the device indicates that the device has moved outside predefined areas, at which point access restrictions are applied and a user password is required to remove those access restrictions. Such a system can be contrasted to that of new independent claim 32 in which different user inputs are required to remove the restrictions on user access in dependence on the determined location information. Ozeki discloses a device in which either a password is required (if the device is deemed to be in a restricted location) or password entry is not required (if the device is deemed to be in a secure location). Ozeki does not disclose using different passwords (i.e. predetermined user inputs) to remove the restrictions once they have been applied, in dependence on the determined location information. In Ozeki, unlike claim 32, once user access restrictions have been actually applied, only a single password is available to remove the restrictions.

As indicated above, the feature of requiring input of a first predetermined password if the device is in a secure location and input of a second predetermined password to unlock the device if it is not in a secure location is neither disclosed in nor suggested by Ozeki in any way.

As described above, Bates determines a geographic-specific password for the current location of the device (based on a list of locally stored geographic-specific passwords for a series of geographic locations), prompts the user for a password, and compares the entered password against the determined geographic-specific password. If the password matches, normal processing continues. If the password does not match, the user is prompted to re-enter the password.

In claim 32, the password required to unlock the mobile device is based on whether the mobile device is determined to be in a secure location or an insecure location. The required password is not strictly limited to the geographic location, but the perceived security of the determined location of the mobile device. This is in contrast to Bates where the password required to unlock the device is a geographic-specific password. Furthermore, there is no description or suggestion in either Fogle or Bates for the feature of determining if the device is in a secure location based on the determined location information.

Therefore, it is submitted that new independent claim 32 is patentable in that the cited references fail to teach or suggest each and every feature recited.

Claim 26

The Examiner has rejected claim 26 under 35 U.S.C 103(a) as being obvious having regard to U.S. Patent No. 6,556,819 (Irvin) in view of U.S. Patent No. 6,002,427 (Kipust). At page 8, the Examiner states that Irvin describes all of the features of claim 26 except for, applying, if the mobile electronic device is determined to be in a secure location, a first countdown timer value defining a duration after which the mobile electronic device will be locked if user interaction with the mobile electronic device is not detected, and applying, if the mobile electronic device is determined not to be in a secure location, a second, shorter, countdown timer value defining the duration after which the mobile electronic device will be locked if user interaction with the mobile electronic device is not detected. The Examiner relies on Kipust as describing this feature at col. 7, lines 19-52.

Irvin describes a security system for a cellular telephone for controlling the status of security features based on location. Upon a triggering event (such as motion detection or a powering on of the phone), if one or more security features have been implemented the phone determines its location (for example, using a GPS receiver) and compares the determined location against a list of safe zones stored in memory. If the phone is in a safe zone, security processing ends and normal operation of the phone resumes. If the phone is not in a safe zone, security measures are initiated such as providing an audio alarm, or activating a secondary security system such as requiring a password (see col. 6, lines 14-42).

Kipust describes a security system that uses a proximity sensor to protect against unauthorized access to a personal computer (PC). The proximity sensor detects changes in heat, movement or other physical changes indicating user departure from an established vicinity of the PC (col. 3. line 66 to col. 4, line 1). The proximity sensor transmits a proximity signal to a controller which controls operation of the security system 100 (col. 4, lines 35-37). The controller waits a pre-programmed amount of time before arming itself upon detection by the proximity sensor that the user has departed the work area. The amount of time may be set by the user to ensure that the departure is for a longer duration and to take into account the security needs of a particular PC. Thus, stricter security needs can be met with a smaller pre-programmed amount of time (see col. 3, lines 24-30).

The signal generated by the proximity sensor is compared against a sensitivity setting to generate an activity signal. The sensitivity setting is selected by the user to adjust the sensitivity or range of the proximity sensor. This allows the vicinity in which activity is detected to be varied depending upon the security needs and environment of the secured PC. The level or type of signal required to generate the activity signal can be dynamically changed to account for differing levels of activity at different times of the day or different days of the week. If the activity signal indicates that activity has ceased then a count down procedure is performed to wait a pre-programmed amount of time before arming the security system (col. 7, lines 31-56). Once armed, the security system transmits an appropriate signal to the PCT to invoke certain security measures such as clearing the screen of the information being displayed, invoking a screen saver and/or ignoring input from input devices such as keyboard or pointing device.

While Irvin describes determining if the device is in a secure location based on location information, it does not describe applying different security settings depending on whether the device is in a secure location or an insecure location. In Ivrin, if the device is in a secure location, security features are disabled. If the device is not in a secure location, security features are enabled. This is in contrast to the claimed invention where different security settings are applied in relation to a particular security feature (i.e., device lockout timer in claim 26) depending on whether the current location is determined to be secure or insecure. While Kipust describes the possibility of different lengths of count down timers prior to arming the system based on security demands, it does not describe, nor suggest changing the count timer based on the determined location of the device. The device in Kipust is a personal computer which does not change in location except for exceptional circumstances unlike a mobile device, thus location information is not important in Kipust, nor is it described in any way. In addition, the proximity sensor detects heat, movement or other physical changes indicating user departure. It does not detect interaction with the PC in terms of user input or the like in contrast to the claimed invention. Furthermore, Kipust is in a non-analogous art in that relates to personal computers rather than mobile communication devices, and involves an external security system having a proximity sensor. The claimed invention provides an integrated solution for a mobile communication device.

Therefore, it is submitted that amended independent claim 26 is patentable in that the cited references fail to teach or suggest each and every feature recited.

New claims

Claims 29 to 34 have been added. Claims 29 and 33 have been added to more fully claim the present application by adding the differential countdown timer of claim 26 as a dependent feature of independent claims 15 and 32. Support for claims 29 and 33 can be found in the claims as originally filed and in the description. Claim 31 is a new independent claim directed to a mobile device for implementing the method of claim 26 and is therefore considered to be patentable for at least the same reasons given for claim 26. Claims 30 and 34 add the limitation that the second predetermined password used when the determined location is not a secure location is more complex than the first predetermined password used when the determined location is a secure location. Support for this limitation can be found at paragraphs [0041], [0044] and [0045] of the specification as originally filed. No new matter has been added by the present amendments.

Related application

The Applicant notes that a continuation application has been filed in respect of former claims 1 to 14 which were cancelled by way of the Applicant's amendment of August 21, 2006. The continuation application has been granted serial no. 11/687,354 and is identified by attorney docket number 42783-0398.

In view of the foregoing remarks and submissions, the Applicant respectfully requests reconsideration and submits that the present application is in condition for allowance. Should the Examiner have any questions in connection with the Applicant's submissions, please contact the undersigned.

Respectfully Submitted,

RESEARCH IN MOTION LIMITED

By /SM/
Stephen Martin
Registration No. 56,740
Telephone (416) 865-3503
Fax (416) 362-0823

Date: October 1, 2007